Remarks/Arguments

Claims 1, 4-25, 28-41, 48-50 are pending in this application. Claims 2, 3, 26 and 27 have been cancelled without prejudice. Claims 42-47 were subject to a restriction requirement and have also been cancelled without prejudice. Claims 1, 16-18, 25, 36 and 38-41 have been amended. No new matter is added by these amendments, nor have these amendments been made for any reasons related to patentability or to overcome any rejections made by the examiner. These amendments merely reflect applicant's desire to more distinctly point out and claim the subject matter the applicant regards as his invention. Additionally, claims 1, 22 and 25 have been amended to overcome the 35 USC § 112 rejections, as discussed below.

I.   Rejections under 35 USC §112

Claim 1 is rejected under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention, in particular because the term "a first secure bitstream" lacked antecedent basis. Claim 1 has been amended to correct the insufficient antecedent basis noted by the Examiner. The Applicant has also noted and corrected a similar antecedent basis issue in claim 25. These amendments do not narrow the scope of the claims.

Claim 22 is rejected under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention, in particular because the term "the FPGA" lacked antecedent basis. Claim 22 has been amended to correct the insufficient antecedent basis noted by the Examiner. This amendment does not narrow the scope of the claims.

II.   Rejections under 35 USC §102

Claims 1, 4-5, 9, 11, 13, 25, 28, 33, 35 and 37 stand rejected under 35 USC §102, as being anticipated by Lawman (U.S. Patent 6,028,445).

"[A] claim is anticipated if each and every limitation is found either expressly or inherently in a single prior art reference." Celeritas Techs., Ltd. v. Rockwell Int'l. Corp., 150 F.3d 1354, 1361, 47 U.S.P.Q.2d 1516, 1522 (Fed. Cir. 1998). The standard for lack of novelty,

9

that is, for "anticipation," is one of strict identity between the prior art reference and the claims. Trintec Indus., Inc. v. Top-U.S.A. Corp., 295 F.3d 1292, 1296, 63 U.S.P.Q.2d 1597, 1600 (Fed. Cir. 2002). In the present Office Action, the Examiner's rejection is based on the Lawman reference, which fails to show all of the elements of the claimed invention.

The Lawman reference is very different from what is claimed in this patent application. Lawman discloses methods for configuring a user-supplied program onto an FPGA. The invention of claims 1 and 25, however, claims "fabricating a first plurality of FPGA integrated circuits" and "fabricating a second plurality of FPGA integrated circuits" (emphasis added). Fabrication is the process of manufacturing the physical FPGA hardware structure (e.g. making the FPGA chip). Configuration is the process of programming an already-fabricated FPGA hardware structure with the software (e.g. bitstream) for a particular function or functions (e.g. programming the FPGA). Configuration is typically performed by a customer or end user, after the FPGA has been physically manufactured. Thus the methods disclosed in Lawman bear no relationship to the methods claimed in this application.

Lawman teaches configuring a first portion of a single FPGA integrated circuit into a data decompression decoder (or alternatively a command interpreter), and then use that configured data decompression decoder to decompress a configuration bitstream and configure a second portion of the FPGA with the decompressed bitstream. See Lawman, col. 3, lines 6-22. This method is performed every time the FPGA integrated circuit is powered up, thus it is performed by the end user. See Lawman, col. 5, lines 39-44.

Claims 1 and 25, on the other hand, claim using mask sets to embed cryptographic key values into the physical FPGA structure as it is being fabricated. Different pluralities of FPGA integrated circuits are embedded with different key values during fabrication, such that a secure bitstream generated using the first secret key will properly configure the first plurality of FPGA integrated circuits but not the second. This method is performed at fabrication time, not at configuration time.

Furthermore, Lawman does not disclose the generation of secure bitstreams, as required by claims 1 and 25. Lawman merely discloses decompressing compressed bitstreams. Compressed bitstreams are not secure, they are merely compressed to save on storage space, using a compression algorithm. Anyone with access to the compression algorithm (which are

10

typically freely distributed, and not kept secure) can decompress and use the compressed bitstream.

Claims 4, 5, 9, 28, 29 and 33 are similarly not anticipated by the Erickson reference. Claims 4, 5 and 9 depend from claim 1, and claims 28, 29 and 33 depend from claim 25. Since the independent claims 1 and 25 are not anticipated by Lawman, as discussed above, neither are these dependent claims. Furthermore, the passage in Lawman recited by the Examiner, col. 7, lines 25-45, relates to the configuration of different areas of a single FPGA chip, at different times. Claims 4 and 28, however, refer to fabrication of two separate pluralities of FPGA integrated circuits, each of which are assigned to a different geographic area of the planet Earth. See Application, paragraph [0083]. Claims 5, 9, 29 and 33 refer to fabrication of two separate pluralities of FPGA integrated circuits, which are fabricated at different moments in time. See Application, paragraph [0083]. Thus the Lawman reference fails to teach or suggest the additional limitations of claims 4, 5, 9, 28, 29 and 33.

Claims 11 and 35 are similarly not anticipated by the Lawman reference. Claim 11 depends from claim 1, and claim 35 depends from claim 25. Since the independent claims 1 and 25 are not anticipated by Lawman, as discussed above, neither are these dependent claims. Furthermore, neither the cited passages in Lawman nor any other portion of the Lawman reference teaches or suggests the claimed limitation of "wherein there are random differences between artwork" implemented by the masks used to fabricate the two pluralities of integrated circuits claimed, in addition to the different embedded secret keys in each plurality. The cited passage in Lawman merely teaches that the user logic configured as a configuration port may be reconfigured to perform other functions once the configuration of the FPGA is completed. This passage says nothing about the FPGA fabrication process at all, much less teaching anything about the claimed limitation of "wherein there are random differences between artwork".

Claims 13 and 37 are similarly not anticipated by the Lawman reference. Claim 13 depends from claim 1, and claim 37 depends from claim 25. Since the independent claims 1 and 25 are not anticipated by Lawman, as discussed above, neither are these dependent claims. Furthermore, neither the cited passages in Lawman nor any other portion of the Lawman

11

reference teaches or suggests the claimed limitation of "wherein the first secret key is embedded by setting an initial state of a selection of memory cells in a device configuration memory" stored in the integrated circuit (such as an FPGA). The passage of the Lawman reference cited by the Examiner is discussing the configuration of a portion of an FPGA, whereas claims 13 and 37 claim "wherein the first secret key is embedded by setting an initial state of a selection of memory cells in a device configuration memory" during fabrication of the FPGA integrated circuits.

Therefore, claims 1, 4-5, 9, 11, 13, 25, 28, 33, 35 and 37 are not anticipated by the Lawman reference. The applicant respectfully requests that the rejections of these claims be withdrawn.

III.   Rejections under 35 USC §103

Claims 7, 8, and 31-32 are rejected under 35 USC § 103 as being unpatentable over Lawman.

Case law makes clear that "the best defense against hindsight-based obviousness analysis is the rigorous application of the requirement for a showing of a teaching or motivation to combine the prior art references." Ecolochem, Inc. v. Southern California Edison Co., 227 F.3d 1361, 1371, 56 U.S.P.Q.2d 1065, 1073 (Fed. Cir. 2000). The absence of a convincing discussion of the specific sources of the motivation to combine the prior art references is a critical omission in the Examiner's obviousness analysis, which mainly discusses the way that the Lawman reference can be combined with the other cited references, or unspecific general knowledge to read on the claimed invention.

Combining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor's disclosure as a blueprint for piecing together the prior art to defeat patentability, the essence of improper hindsight. In re Rouffet, 149 F.3d 1350, 1357, 47 U.S.P.Q.2d 1453, 1456 (Fed. Cir. 1998).

A determination of motivation to support an obviousness rejection requires a factual finding that a skilled artisan has knowledge of the principle of the invention. To render a claim obvious "the reasons why one of ordinary skill in the art would have been motivated to select the references and to combine them to render the claimed invention obvious" must be identified

12

specifically. In re Rouffet, 149 F.3d 1350, 1359, 47 U.S.P.Q.2d 1453, 1459 (Fed. Cir. 1998). In the present Office Action, the Examiner's rejection is based on the Lawman reference in view of the other cited references or the unspecific general knowledge, which fails to show the motivation for combining elements of the instant invention.

Claims 7-8 and 31-32 are not obvious in light of the Lawman reference, because they depend from independent claims that are neither anticipated by nor obvious in light of the Lawman reference. Claims 7 and 8 depend from claim 1, and claims 31-32 depend from claim 25. Since the independent claims 1 and 25 are not anticipated by Lawman, as discussed above, neither are these dependent claims. Furthermore, the Examiner has not cited to any prior art reference which in combination with Lawman would teach all of the limitations of claims 7-8 or 31-32. Thus it appears that the Examiner is relying merely upon some sort of vague, unspecific general knowledge. Neither the Lawman reference nor this unspecified general knowledge provide any motivation to combine Lawman with the general knowledge, to reach the claimed inventions. Thus the Examiner's obviousness rejections comprise an improper hindsight analysis.

Claims 7 and 31 claim the concept of allocating FPGAs to different customers, with each customer having FPGAs with a different key. This allocation scheme makes it difficult for a pirate to obtain FPGAs which will run a pirated bitstream belonging to the first customer, because the bitstream will only run on FPGAs having the first key, and those FPGAs are only sold to the first customer, not to the pirate. The Lawman reference does not teach any type of allocation of FPGAs with different keys to different market segments, whether by geographic area or by customer. Furthermore, there is no motivation to combine Lawman with any other reference, including the unspecific general knowledge cited by the Examiner, to reach the claimed method. Furthermore, Lawman does not even teach any sort of cryptographic key storage memory, as claimed by claims 7 and 31, nor does Lawman even discuss cryptography or securing bitstreams at all. Even if the Lawman reference could somehow be construed to teach an FPGA having a key storage area, this does not supply any motivation to use that supposed feature in the way claimed in claims 7 and 31. Thus claims 7 and 31 are not obvious over Lawman, even in combination with the unspecific general knowledge.

13

As to claims 8 and 32, as discussed above, these claims depend from parent claims 5 and 29, which are not anticipated by the Lawman reference, therefore dependent claims 8 and 32 are likewise not anticipated nor rendered obvious by the Lawman reference. Furthermore, Lawman does not even teach anything about fabrication of FPGAs, as claimed by claims 7 and 31, nor does Lawman even discuss cryptography or securing bitstreams at all. Thus claims 7 and 31 are not obvious over Lawman, even in combination with the unspecific general knowledge.

Claims 6, 10, 30 and 34 stand rejected over Lawman in view of Kean (US Patent 6,292,018).

Turning to claims 6 and 30, these claims recite a method where "only one mask differs between the first and second mask sets." The Examiner contends that the Kean reference discloses a method where only one mask differs between a first and a second mask set. The instant application is claiming mask sets used in the manufacturing process for integrated circuits. The mask sets claimed in the instant application are sets of masks used to fabricate integrated circuits, according to standard circuit manufacturing processes. See, e.g. paragraphs [0010]-[0011], [0082]-[0084], [0101]-[0104]. These mask sets are applied to a silicon wafer to imprint a pattern on the wafer that corresponds to the pattern on the masks within the mask set.

The Kean reference has absolutely nothing to do with masks used to fabricate integrated circuits. The Kean reference at column 30, lines 33-60 is discussing a mask register. Mask registers are registers within an active circuit which contain a series of bits that are used to mask out certain bits from an incoming data value, such as a value loaded on the internal data bus 162 of Kean. The masking function performed by the mask registers is a logical data operation wherein a data value is logically AND'ed with a corresponding value in the mask register. This has the effect of eliminating or masking out any data value that corresponds to a corresponding mask value of '0'. There is no relationship between the mask register of Kean and the mask sets of the instant application. Even if the mask register of Kean were combined with the FPGA of Lawman, this combination would totally fail to teach a method of fabricating FPGAs "wherein only one mask differs between first and second mask sets." Furthermore, the mask register of Kean is from a totally different field of technology than the mask sets of the instant application, thus there is no motivation to combine these two totally different concepts, even if such a combination would read on claims 6 and 30, which it does not. Furthermore, as discussed above,

14

the Lawman reference teaches configuration of FPGAs, not fabrication of FPGAs, and thus Lawman in combination with Kean would still have nothing to do with the claims 6 and 30, which are about fabrication of FPGAs.

Turning to claims 10 and 34, these claims depend from claims 6 and 30, respectively . The Lawman reference, even in combination with the Kean reference, fails to teach the method of parent claims 6 and 30, as discussed above, thus they also fail to teach the methods of claims 10 and 34. Thus claims 6, 10, 30 and 34 are not obvious in light of Lawman and Kean.

Claims 12, 16, 18-21 and 36 stand rejected over Lawman in view of Erickson (US Patent 6,212,639).

Claims 12 and 36 are not rendered obvious by the Lawman and Erickson references. Claim 12 depends from claim 1, and claim 36 depends from claim 25. Since the independent claims 1 and 25 are not anticipated by Lawman, as discussed above, these dependent claims are not obvious, because the elements of the parent claims 1 and 25 are not taught by nor obvious over Lawman or Erickson.

Claim 16 and 39 are similarly not rendered obvious by the Lawman and Erickson references. Claim 16 depends from claim 1, claim 39 depends from claim 25. Since the independent claims 1 and 25 are not anticipated by Lawman, as discussed above, these dependent claims are not obvious over Lawman and Erickson. Furthermore, the Erickson reference does not teach "wherein an unencrypted bitstream is loadable into one of the first plurality of FPGA integrated circuits" as claimed. Erickson teaches encrypting the configuration data prior to loading it into the FPGA. See Erickson, 3:31-42, 4:15-39.

Turning to claims 18-21, the Examiner contends that the Lawman reference teaches "embedding a first secret key within the artwork of an FPGA integrated circuit", citing to col. 7, lines 20-45 and col. 8, lines 12-63, which discuss the decompression decoder. Contrary to the Examiner's contention, however, this cited passage in Lawman is discussing how the decompression decoder is configured into the user logic of the FPGA when the FPGA is configured by the end user, and is totally unrelated to fabrication of the FPGA integrated circuit structure itself, as claimed in claim 18.

The Examiner also contends that Lawman teaches storing keys in encrypted bitstreams, and decrypting encrypted bitstreams using a key embedded in the artwork of an FPGA. Contrary

15

to the Examiner's contention, however, Lawman totally fails to teach anything about encrypted bitstreams, nor about the use of keys for any function, including encrypting or decrypting bitstreams. Lawman discusses compressed bitstreams, but compressed bitstreams are not secure, therefore they are very different from encrypted bitstream, which are secure.

The Examiner also contends that the Erickson reference supplies the teachings for "setting up a secure network link between the FPGA and a server using the user-defined second secret key." This cited passage in Erickson teaches the implementation of a public key system to encrypt the data being transferred from the storage device 120 to the PLD 110. This teaching is expressly teaching away from the method claimed in the instant application. In a public key system, there are no keys stored in the encrypted data being transferred. To receive an encrypted data stream, the receiving unit (here the PLD 110) sends its own public key to the sending unit (here the storage device 120). The storage device 120 uses this public key to encrypt the configuration data, and then sends the encrypted configuration data to the PLD 110. No keys are included in this encrypted configuration data. The PLD 110 then uses its private key to decrypt the encrypted configuration data, and loads it into the PLD memory.

In contrast, the method of claims 18-21 claim storing a second key within an encrypted FPGA bitstream, using a first key to decrypt the encrypted FPGA bitstream to recover the second key, and then using the recovered second key to set up a secure network link between the FPGA and a server. An embodiment of these claims is discussed at paragraphs [0148] to [0151]. Thus even if Lawman somehow could be construed to teach some of the limitations of claim 18, there is no motivation to combine Lawman with Erickson to render claim 18 obvious, because Erickson directly teaches away from claim 18. Thus the Lawman and Erickson references do not anticipate nor render obvious claim 18, nor its dependent claims 19-21.

Claims 14-15, 17 and 38 stand rejected over Lawman in view of Plants (US Patent 6,560,743).

Turning to claims 14-15 and 38, these claims, dependent on claims 1 and 25 respectively, recite a method wherein a key is extracted from a larger set of data values by using a CRC algorithm to extract the key. The Examiner contends that Lawman teaches the limitations of the parent claims 1 and 25. As discussed above, the configuration methods taught by Lawman are totally unrelated to the fabrication methods claimed in claims 1 and 25. Therefore Lawman fails

16

to anticipate claims 1 and 25 and thus claims 14-15, and 38 are not obvious over Lawman and Plants.

Furthermore, the Examiner contends that Plants discloses using "a CRC circuit to make sure the correct data is received." The Examiner is correct as to what Plants discloses. However, as the Examiner concedes in the current office action, Plants does not disclose the subject matter of claims 14-15 and 38. Simply put, Plants discloses the conventional use of a CRC circuit to verify the correctness of received data, by comparing a known value included with the data to a signature derived from the data by the CRC circuit. See Plants, (7:58-63). Plants does not use a CRC algorithm to extract a key from a larger set of data values. In the instant application, the CRC algorithm is used for the novel purpose of extracting the key by summarizing the larger set of data values into the smaller key. The extracted key is not compared with anything, nor is it used to verify the correctness of any data. Rather the extracted key is used to encrypt or decrypt data. Thus Plants does not teach the extraction of a key using a CRC algorithm, as claimed in claims 14-15 and 38, and therefore the combination of Lawman and Plants fails to teach or even suggest the inventions of claims 14, 15 and 38. The rejections should therefore be withdrawn.

Turning to claim 17 and claim 40,[1] the Examiner contends that Plants teaches the implementation of a Message Authentication Code (MAC) to check the validity of a data stream in an FPGA, and this in combination with Lawman renders claim 17 obvious. However, as discussed above and as the Examiner concedes in the current office action, Plants teaches the use of a CRC, which is different from a MAC. A CRC does not provide protection against deliberate alteration of the data stream, whereas a MAC does.

A CRC merely provides protection from an accidental alteration of the data stream, for example by a transmission error. The CRC check is run on the data, and if the computed CRC value is different from the CRC value supplied with the data stream, then the data contains an error. However, if someone wants to intentionally alter data, for example to remove a copyright notice, this person merely has to alter the data, compute the new CRC value, and append that new CRC value to the data being transmitted. This intentionally altered data, along with the

---

[1] The Examiner cites no specific reasons for rejecting claim 40, but claim 40 is discussed here because the same arguments apply to claim 40 as claim 17.

DOCSOC1:171291.1

altered CRC, will not be detected as erroneous, because the CRC check run on the altered data will return the same value as the altered CRC supplied with the data.

With a MAC, however, the person altering the data cannot also make corresponding alterations to the MAC. Unlike a CRC, a MAC is generated using a secret key, such as the key embedded in the FPGA as claimed in claims 17 and 40, and applying that key to the data to be protected by the MAC. Thus the MAC is specific to the unaltered data stream, and is tied to the secret key. If the data is altered, for example intentionally to remove a copyright notice, or unintentionally by a transmission error, then the data will not match the MAC, and the FPGA will reject the data. A pirate wishing to alter the data must also alter the MAC, or else the data will not be accepted by the FPGA. However, altering the MAC requires access to the secret key, which the pirate will not have. Thus, Erickson, even in combination with Plants, fails to teach the use of a MAC as claimed in claims 17 and 40, and the rejection should be withdrawn.

Turning to claims 22-24, and 48-50, the Examiner has rejected these claims over Lawman in view of Candelore. Initially, as discussed above with reference to prior claims, Lawman totally fails to disclose storing any sort of key information on an FPGA chip. Additionally, the Examiner recognizes that Lawman fails to teach "causing the FPGA to calculate a message authentication code (MAC) corresponding to a user design," and "storing the message authentication code with bitstream information in a nonvolatile memory." The Examiner contends that Candelore teaches "the generation of the MAC and storage device for keeping necessary info to receive the contents data and authentication data (Col 4 lines 45-64)."

However, as the Examiner concedes in the current office action, neither the cited passage of Candelore nor any other teaching of Candelore mentions applying any of Candelore's teachings to FPGAs, or to bitstreams for configuring FPGAs, as required by claims 22-24 and 48-50. Candelore discusses using a microprocessor to implement the access control teachings of Candelore, not an FPGA. Thus, Candelore, even in combination with Lawman, does not cause an FPGA to calculate a message authentication code, nor does Candelore store a message authentication code with bitstream information. Furthermore, since the Lawman reference is from the field of FPGAs, and the Candelore reference is unrelated to FPGAs, there is no motivation to combine these two references from unrelated fields. Accordingly, the rejections of claims 22-24 should be withdrawn.

18

The Examiner has not supplied any grounds for rejection of claim 41. Nevertheless, this claims is similarly not anticipated by the Lawman reference. Claim 41 depends from claim 25. Since the independent claim 25 is not anticipated by Lawman, as discussed above, neither is this dependent claim. Furthermore, neither the Lawman nor Erickson references, nor any of the other cited references, teach "downloading a secure programmable integrated circuit bitstream through a network" as claimed. As conceded by the Examiner in this office action, the passage from Erickson cited in the prior office action is discussing a "daisy-chain" approach to configuring multiple PLD's on the same circuit board, using a direct wire connection. (9:44-45; FIG. 4) The "secure communications link" referred to by the Erickson reference is not a "network" as claimed, rather it is a conventional "bus" or "daisy-chain" connection between a configuration memory and a number of PLDs on the same board. (9:51-10:2).

IV. Conclusion

The claims of this application are neither anticipated nor obvious over any of the cited references, either alone or in combination. Therefore, prompt allowance of these claims is earnestly requested. Should the Examiner have any questions or comments, the undersigned can be reached at (949) 567-6700.

The Commissioner is authorized to charge any fee which may be required in connection with this Amendment to deposit account No. 15-0665.

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

Dated: January 23, 2006

By: _Donald Daybell_____

Donald Daybell
Reg. No. 50,877

Orrick, Herrington & Sutcliffe LLP
4 Park Plaza, Suite 1600
Irvine, CA 92614-2558
Tel. 949-567-6700
Fax: 949-567-6710

19